

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平8-507416

(43) 公表日 平成8年(1996)8月6日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	
H 0 4 L 9/32				
G 0 6 F 15/00	3 3 0 Z	9364-5L		
G 0 9 C 1/00		7259-5 J		
		8842-5 J		
			H 0 4 L 9/00	A

審査請求 未請求 予備審査請求 有 (全 36 頁)

(21) 出願番号 特願平6-511416  
 (86) (22) 出願日 平成5年(1993)11月2日  
 (85) 翻訳文提出日 平成7年(1995)5月8日  
 (86) 国際出願番号 P C T / U S 9 3 / 1 0 5 8 5  
 (87) 国際公開番号 W O 9 4 / 1 0 7 7 8  
 (87) 国際公開日 平成6年(1994)5月11日  
 (31) 優先権主張番号 9 7 0 , 6 1 1  
 (32) 優先日 1992年11月3日  
 (33) 優先権主張国 米国 (U S)

(71) 出願人 ノーヴェル・インコーポレーテッド  
 アメリカ合衆国 84601 ユタ州・プロヴ  
 オ・イースト 1700 サウス・122  
 (72) 発明者 キングドン, ケヴィン  
 アメリカ合衆国 84057 ユタ州・オーレ  
 ム・イースト 600 ノース・1331  
 (74) 代理人 弁理士 山川 政樹 (外5名)

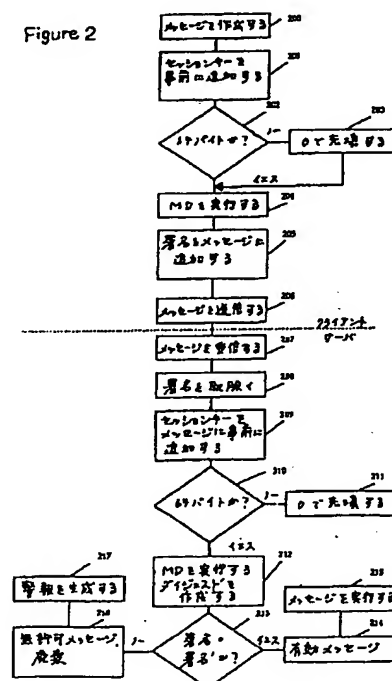
最終頁に続く

(54) 【発明の名称】 クライアントサーバ通信の認証のための方法及び装置

## (57) 【要約】

本発明は、メッセージパケットの偽造を防止するためのメッセージパケット認証の方法及び装置を提供する。そこで、署名と呼ばれるメッセージダイジェストの一部分を、実際のメッセージがワイヤを介して送信されるときに実際のメッセージに追加する(205)。受信局はメッセージから署名を取り除き(208)、同じ秘密セッションキーを事前に追加し(209)、それ独自のメッセージダイジェストを作成する(212)。受信局により作成されたダイジェストの署名を送信局により追加されたダイジェストの署名と比較する(213)。一致があれば、認証メッセージを想定する(214)。一致がなければ、メッセージを無効と考え、廃棄する(216)。

Figure 2



## 【特許請求の範囲】

1. センダとレシーバとの間で伝送されるメッセージを認証する方法において、前記センダでメッセージを生成する過程と；

前記メッセージとセッションキーを組合わせて、第1の追加メッセージを作成する過程と；

前記第1の追加メッセージの第1のダイジェストを計算する過程と；

前記第1のダイジェストの第1の部分を前記メッセージと組合わせて、送信メッセージを作成する過程と；

前記送信メッセージを前記レシーバへ送信する過程と；

前記送信メッセージから前記第1のダイジェストの前記第1の部分を取り除き、その結果として前記メッセージを得る過程と；

前記セッションキーを前記メッセージと組合わせて、第2の追加メッセージを生成する過程と；

前記追加メッセージの第1のダイジェストを計算する過程と；

前記第1のダイジェストの前記第1の部分と前記第2のダイジェストの第2の部分とを比較する過程と；

前記第1のダイジェストの前記第1の部分が前記第2のダイジェストの前記第2の部分と一致したときに前記メッセージを認証する過程とから成る方法。

2. 前記センダはクライアント/サーバネットワークの中のクライアントである請求項1記載の方法。

3. 前記レシーバはクライアント/サーバネットワークの中のサーバである請求項1記載の方法。

4. 前記第1の追加メッセージの第1のダイジェストを計算する前記過程は、前記第1の追加メッセージについてダイジェストアルゴリズムを実行することにより実行される請求項1記載の方法。

5. 前記ダイジェストアルゴリズムはMD4ダイジェストアルゴリズムである請求項4記載の方法。

6. 前記第1のダイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記センダの現在状態を初期状態として使用する請求項4記載

の方法。

7. 前記第2のダイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記現在状態を初期状態として使用する請求項6記載の方法。

8. 前記現在状態は認証されたメッセージが受信されるときに進む請求項7記載の方法。

9. 前記現在状態は認証されたメッセージが受信されないときには進まない請求項8記載の方法。

10. 前記セッションキーは：

乱数列呼掛けを前記センダに対し実行する過程と；

前記センダのユーザからパスワードを要求する過程と；

前記パスワードから第1のパスダイジェストを生成する過程と；

前記第1のパスダイジェストと前記呼掛けをバッファにおいて組合わせる過程と；

前記バッファのバッファダイジェストを生成する過程と；

前記セッションキーを前記バッファダイジェストの第1の数のバイトとして定義する過程とにより生成される請求項1記載の方法。

11. センダとレシーバとの間で伝送されるメッセージを認証する装置において、

前記センダでメッセージを生成する手段と；

前記メッセージとセッションキーを組合わせて、第1の追加メッセージを作成する手段と；

前記第1の追加メッセージの第1のダイジェストを計算する手段と；

前記第1のダイジェストの第1の部分を前記メッセージと組合わせて、送信メッセージを作成する手段と；

前記送信メッセージを前記レシーバへ送信する手段と；

前記送信メッセージから前記第1のダイジェストの前記第1の部分を取り除き、その結果として前記メッセージを得る手段と；

前記セッションキーを前記メッセージと組合わせて、第2の追加メッセージを生成する手段と；

前記第2の追加メッセージの第2のダイジェストを計算する手段と；

前記第1のダイジェストの前記第1の部分と、前記第2のダイジェストの第2の部分とを比較する手段と；

前記第1のダイジェストの前記第1の部分が前記第2のダイジェストの前記第2の部分と一致したときに前記メッセージを認証する手段とを具備する装置。

12. 前記センダはクライアント/サーバネットワークにおけるクライアントである請求項11記載の装置。

13. 前記レシーバはクライアント/サーバネットワークにおけるサーバである請求項11記載の装置。

14. 前記第1の追加メッセージの前記第1のダイジェストは、前記第1の追加メッセージについてダイジェストアルゴリズムを実行することにより計算される請求項11記載の装置。

15. 前記ダイジェストアルゴリズムはMD4ダイジェストアルゴリズムである請求項14記載の装置。

16. 前記第1のダイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記センダの現在状態を初期状態として使用する請求項14記載の装置。

17. 前記第2のダイジェストを作成するために前記ダイジェストアルゴリズムを実行するときに前記現在状態を初期状態として使用する請求項16記載の装置。

18. 前記現在状態は認証されたメッセージが受信されたときに進む請求項17記載の装置。

19. 前記現在状態は認証されたメッセージが受信されないときには進まない請求項18記載の装置。

20. セッションキーを生成する手段であって；

乱数列呼掛けを前記センダに対し実行する手段と；

前記センダのユーザからパスワードを要求する手段と；

前記パスワードから第1のパスダイジェストを生成する手段と；

前記第1のパスダイジェストと前記呼掛けとをバッファにおいて組合わせる手

段と；

前記バッファのバッファダイジェストを生成する手段と；

前記セッションキーを前記バッファダイジェストの第 1 の数のバイトとして定

義する手段とを具備する手段をさらに含む請求項 11 記載の装置。

## 【発明の詳細な説明】

クライアントサーバ通信の認証のための方法及び装置発明の分野

本発明はネットワーク通信の分野に関する。

背景技術

データ、アプリケーション、ファイル、処理パワー、通信並びにプリンタ、変復調装置、大容量記憶装置などの他の資源の共用を可能にするために、パーソナルコンピュータ又はワークステーションをコンピュータネットワークを介して連係できる。一般に、資源の共用はネットワークサーバの使用によって実行される。サーバは集中型資源を管理し、データを管理し、及び多くの場合に「クライアント」と呼ばれる他のPCやワークステーションとの資源を共用するのに専用に用いられる処理装置である。サーバと、ネットワークと、PC又はワークステーションとは、一体に組合わされて、クライアント/サーバコンピュータネットワークを構成する。クライアント/サーバネットワークモデルの1例を図1に示す。

図1は、サーバマシン102に結合するクライアントマシン101を示す。クライアントマシン101はPC、ワークステーションなどであれば良い。サーバマシンは、ファイルを記憶する大容量記憶装置を含む専用プロセッサ、PC、ワークステーションなどであれば良い。典型的には、大容量記憶装置はディスクドライブ又は他の適切な装置である。

クライアントマシン101は、クライアントスタブ103と通信するクライアント102から構成されている。クライアントスタブ103はトランスポートエンティティ104と通信する。サーバマシン105はサーバ106と、サーバスタブ107と、トランスポートエンティティ108とを含む。

クライアントマシン101に関して説明すれば、クライアント102はサーバのファイルを利用する局所プロセッサである。クライアントスタブ103は、クライアントがサーバをアクセスすることを可能にする局所手続きの集合体である。トランスポートエンティティ104はネットワーク、すなわち、「ワイヤ」109に対するアクセスを実行する。ワイヤ109はクライアントとサーバとの間

の通信媒体を表わし、実際のバードワイヤード通信媒体であっても良く、あるいは、

無線接続であっても良い。同様に、サーバスタブ107はサーバがクライアントと通信することを可能にする手続きの集合体であり、トランスポートエンティティ108はサーバからワイヤ109へのアクセスを実行する。

動作中、クライアントとサーバとの通信は(クライアントからの)要求と(サーバからの)応答という形態をとる。この通信は遠隔手続き呼出しの形態である。クライアントは1つの手続きを呼出し且つ結果を獲得するアプリケーションに類似している。その相違点は、手続きが必ずクライアント101と同じマシンにあるとは限らず、むしろサーバマシン105にあるということである。

当初、クライアント102はクライアントマシンのクライアントスタブ103(クライアント102の局所アドレススペースに常駐している)にあるスタブ手続きを呼び出す。クライアントスタブ103はその呼出しからメッセージを構成し、メッセージをトランスポートエンティティ104に提供する。トランスポートエンティティ104はワイヤ109を介してメッセージをサーバマシン105へ通信する。サーバにおいては、トランスポートエンティティ108はメッセージをサーバスタブ107に渡す。そこで、サーバスタブはサーバ106から適切なサーバ手続きを呼び出す。サーバ106はメッセージに関して演算し、次にその手続きと何らかの結果をサーバスタブ107に戻す。サーバスタブ107は応答メッセージを構成し、それをトランスポートエンティティ108に提供する。応答メッセージはワイヤ109を介してクライアントマシン101のトランスポートエンティティ104へ送信される。トランスポートエンティティは応答メッセージをクライアントスタブ103に提供する。クライアントスタブ103は、サーバによって戻された手続きと何らかの値をクライアント102に戻す。

コンピュータネットワークでは、クライアントとユーザが異なる特権のレベルを有する。ユーザの追加、ユーザの削除、パスワードの変更などのいくつかの機能は最高の特権をもつユーザに限定されている。それらのユーザクライアントはネットワーク管理責任者であることが多く、それらのユーザは必要に応じてネッ

トワークを変更することが可能でなければならない。加えて、大半のユーザに対して制約が設けられているある種のファイル又はアクティビティもあるだろう。たとえば、金融データはその金融データを知る又は使用する必要があるユーザに

限定されている場合が多い。一般に、他のユーザはそのデータをアクセスすることを許されない。

クライアント／サーバモデルにおいては、メッセージを「パケット」として転送する。メッセージパケットの1例を図3Aに示す。メッセージは4バイトの長さヘッダー（ローハイ）標識301から構成されている。長さヘッダー301はその後に続くメッセージの長さを識別するもので、次のような情報を含む：

Checksum  
PacketLength  
TransportControl  
HPacketType  
DestinationNet  
DestinationNode  
DestinationSocket  
SourceNet  
SourceNode  
SourceSocket

長さヘッダー301の後に要求コード302が続く。要求コード302はクライアントによって要求されている手続きの特定の型である。要求コード302の後にデータ303が続く。データ303の長さは可変であっても良い。

メッセージパケットの特定の1つの型は「NCPパケット」と呼ばれるが、そのNCPはNetWare Core Protocolを表わしている。（NetWareはユタ州ProvoのNovell, Corporationの商標である）。NetWareはネットワークシステム用オペレーティングシステムである。NCPパケットは長さヘッダーの中に次の追加情報を含む：

packet type



sequence number

connection low

task

connection high

メッセージパケットの標準部分は発信元アドレスと、受信先アドレス及び長さ  
とを始めとして、他の複数の情報を提供する。NCP部分は接続番号と、シーケ  
ンス番号とを含む。ステーション接続番号は活動中のステーションのテーブルへ  
の索引をサーバに与える。サーバは活動ステーションテーブルを使用し、そのス  
テーションのネットワークアドレス及びシーケンス番号を含めた、ステーション  
のセッションに関する情報を追跡する。

接続番号は一部で機密性検査として使用される。サーバは、要求パケットを受  
信するときに、パケットの接続番号をその接続テーブルへの索引として使用する  
。要求パケットのネットワークアドレスは、その要求パケットに含まれている接  
続番号に対応する接続テーブルエントリに記憶されたネットワークアドレスと一  
致していなければならない。これは要求パケットを有効化する1つの方法である  
。

シーケンス番号もパケットを有効化するために使用される。シーケンス番号は  
、サーバとクライアントの双方によって維持されるバイトである。クライアント  
が要求パケットを送信するとき、そのクライアントはシーケンス番号を増分する  
。同様に、サーバは要求パケットを受信するときに、そのクライアントのシーケ  
ンス番号（サーバの接続テーブルに記憶されている）を増分する。シーケンス番  
号はクライアントによって256回目の要求が実行されるたびに（それが1バイ  
トの長さであるために）循環する。

クライアントのシーケンス番号を増分する前に、サーバは既に受信した要求パ  
ケットのリストに照らしてシーケンス番号を検査する。この検査は、サーバが重  
複する要求パケットをサービスしないことを確認するためのものである。シーケ  
ンス番号が重複する要求パケットを指示しない場合、サーバはサーバの接続テー  
ブルに記憶されているシーケンス番号に照らして要求パケットのシーケンス番号

を検査する。それら2つの番号が等しくなければ、サーバはパケットを廃棄する。

それらの予防措置にもかかわらず、時折、ネットワークアドレス、接続局、その局の接続番号及び局のシーケンス番号を検出することによるメッセージパケットの偽造の可能性がある。典型的には、メッセージパケットを偽造する目的は、偽造者の特権レベルを更新できるようにより高い特権をもつユーザ又はクライアントを「模倣する」ことである。偽造者は、通信媒体からネットワークパケット

を捕捉することにより、さらに高い特権をもつ局の接続番号を捕獲できるであろう。それらは、より高い特権をもつ局からサーバへ送信されるネットワークパケットである。偽造者はプロトコル解析ツールを使用してそれらのパケットを捕獲しうるだろう。

接続番号を獲得することによって、偽造者は傍受されたメッセージの中と同じ局接続番号を使用して、メッセージをサーバ受信先アドレスへ送信することによりメッセージを偽造しようと試みるであろう。ところが、それだけでは侵入者がメッセージを偽造することを可能にするには不十分である。先に述べた通り、サーバはシーケンス番号を検査し、それを既に受信した要求のリストと比較する。新たな要求のシーケンス番号はそれと関連して、次に続くシーケンス番号を有しているべきである。有していないのであれば、それは無効の要求であり、サーバはそのパケットを廃棄する。

侵入者はシーケンス番号を「推測する」ことによりメッセージを偽造しようと試みるかもしれない。256の後にシーケンス番号は「循環する」ので、侵入者はシーケンス番号を見出す前に256回の試行を試みるだけで良い。侵入者はサーバからの応答を受信するのではなく、むしろ、サーバからの応答を検出しなければならないか又はサーバへ発行された要求が実行されているか否か（たとえば、侵入者に関わる特権状態の変化）を検出しなければならない。

ネットワーク侵入者に対して可能な解決方法の1つは、侵入者型アクティビティを検出するために使用されるネットワークを監視するというものである。たとえば、正しいシーケンス番号を提供するための試行錯誤の試みが検出されるよう

にネットワークを監視できるであろう。たとえば、シーケンス番号を提供するときのある回数の許容失敗試行を伴ってウィンドウを定義できるであろう。問題は、許容再試行のためのウィンドウの大きさに応じて、侵入者がそのウィンドウの中で無作為に正しいシーケンス番号を得ることもありうるという点である。ウィンドウを小さくすれば、正当なユーザが正しいシーケンス番号を与えないときに正当なトランザクションが中断されてしまうであろう。侵入者のアクセスを単に検出する代わりに、侵入者のネットワークアクセスを防止する方法及び装置を提供することが望まれる。

#### 本発明の概要

本発明は、メッセージパケットの偽造を防止するためのメッセージパケット認証の方法及び装置を提供する。メッセージパケットを作成した後、そのメッセージに秘密セッションキーを事前に追加し、変更したメッセージについてメッセージダイジェスティングアルゴリズムを実行して、メッセージダイジェストを作成する。次に、署名と呼ばれるメッセージダイジェストの一部分を、実際のメッセージがワイヤを介して送信されるときに実際のメッセージに追加する。受信局はメッセージから署名を取り除き、同じ秘密セッションキーを事前に追加し、それ独自のメッセージダイジェストを作成する。受信局により作成されたダイジェストの署名を、送信局により追加されていたダイジェストの署名と比較する。一致があれば、認証メッセージを想定する。一致がないならば、メッセージを無効と考え、廃棄する。本発明の1つの利点は、セッションキーが決してワイヤを介して送信されないことである。受信局（サーバ）は既にキーをもっており、キーをメッセージデータと共に使用して、パケットを受信した時点でメッセージダイジェストを再計算する。NCPセッションの開始中に共用秘密キー（セッションキー）を生成する。加えて、送信局と受信局の双方により累積状態情報を維持しておく。この状態情報もメッセージを認証するために使用される。

#### 図面の簡単な説明

図1は、クライアント／サーバモデルのブロック線図である。

図2は、本発明のセッションキーを使用するメッセージセッションの流れ図で

ある。

図3A～図3Gは、メッセージセッション中のメッセージ構造の図である。

図4は、メッセージセッション中のクライアント状態の流れ図である。

図5は、メッセージセッション中のサーバ状態の流れ図である。

図6は、セッションキーの生成を示す流れ図である。

図7は、セッションキーを認証する方法の流れ図である。

図8は、本発明を実現するコンピュータシステムのブロック線図である。

図9は、本発明のブロック線図である。

#### 発明の詳細な説明

メッセージ認証の方法及び装置を説明する。以下の説明中、本発明をさらに完全に理解させるために、メッセージ型、メッセージ長さなどの特定の詳細な事項を数多く挙げる。しかしながら、それらの特定の詳細がなくとも本発明を実施することは明白であろう。別の場合には、本発明を無用にわかりにくくしないように周知の特徴を詳細には説明していない。

本発明はメッセージごとに、センダを識別し且つ認証する署名を与える。さらに、本発明はセッションに関する状態情報を追跡し、その累積効果を使用して、センダを保護し且つ認証するのを助ける。

本発明の署名方式は「メッセージダイジェスティング」として知られている動作を利用する。メッセージダイジェスティングはデータの保全性を与え且つ誤りを検出するための方式である。使用に際して利用可能なメッセージダイジェスティングアルゴリズムはいくつかあり、そのいくつかはR i v e s t, S h a m i r及びA s s o c i a t e s (R S A) により提供されている。R S AメッセージダイジェスティングアルゴリズムはMD 2, MD 4及びMD 5として知られている。本発明の好ましい実施例は、メッセージダイジェスティングアルゴリズムMD 4から派生したものを利用する。MD 4アルゴリズムは、本明細書にも参考として取り入れられているRFC 1320「The MD 4 Message-Digest Algorithm」, R. Rivest, MIT Laboratory for Computer Science and RSA D

ata Security, Inc. 1992年4月の中で説明されている。本発明の好ましい実施例では、MD4アルゴリズムの中で説明されているパディング方式の代わりに、ここで説明するパディング方式を使用する。しかしながら、本発明はどのような適切なパディング方式と組み合わせても使用可能であろう。加えて、MD2ダイジェスティングアルゴリズムやMD5ダイジェスティングアルゴリズムをダイジェスティングアルゴリズムとして使用しても良い。

ダイジェスティングアルゴリズムの代わりに、本発明の趣旨から逸脱することなく、他の暗号の上で安全である一方方向ハッシングアルゴリズムを使用しても良い。ハッシュ関数は、値を広い定義域からより小さな範囲にマッピングする数学的関数である。好ましい実施例では、ハッシュ関数はその関数を定義域内の1組の値に適用した結果がその範囲にわたって一様に（且つ見かけは無作為に）分布するようなものである。この方式を使用すると、時間を節約しつつ、依然として有効なデジタル認証署名の利点を発揮するように、メッセージの暗号化を回避することができる。

#### メッセージ署名

メッセージを認証するために署名を作成し且つ利用する方法を図2の流れ図に示す。ステップ200では、クライアントによりメッセージを作成する。このメッセージは図3Aに示すようなものである。メッセージは4バイトの長さヘッダー（ローハイ）標識301から構成されている。長さヘッダー301はその後に続くメッセージの長さを識別し、発信元と受信先の情報を含む。長さヘッダー301の後に要求コード302が続く。要求コード302は、クライアントにより要求されている特定の型の手続きである。要求コード302の後にデータ303が続いている。データ303の長さは可変であっても良い。

ステップ201では、以下に詳細に説明するようにして作成されるセッションキーをメッセージに事前に追加する。図2のステップ201のセッションキーの事前追加を図3Bに示す。8バイトのキー304は長さ標識301の前でメッセージに事前追加される。

決定ブロック202では、引き数「64バイトか？」を形成する。引き数が偽

である場合、すなわち、メッセージが 64 バイトを有していない場合、システムはステップ 203 へ進み、メッセージの残り部分を零で充填する。これは図 3B のパディング 305 である。好ましい実施例においては、必要に応じてパディング 305（複数の零から構成されている）がメッセージの終わりに追加されるように、メッセージダイジェストアルゴリズムは演算に際して 64 バイトを要求する。要求コードとデータを合わせて 64 バイトであり、4 バイトの長さは合わせて 64 バイトに対してセッションキーの 8 ビットの中で指示されている。

ステップ 203 の後、すなわち、決定ブロック 202 における引き数が真であれば、システムはステップ 204 へ進む。ステップ 204 では、事前追加メッセージからメッセージダイジェストを生成するためにメッセージダイジェストアルゴリズムを実行する。メッセージダイジェストアルゴリズムの実行は図 3C の 1

6 バイトのメッセージダイジェストを作成する。

ステップ 205 では、ダイジェストの初めの 8 バイト、すなわち、署名 306 をメッセージに追加する。これを図 3D に示す。8 バイトの署名 306 は実際の NCP データの終わりに追加される。メッセージをワイヤを介して送信するにはパディングは不要である。ステップ 206 では、メッセージをサーバへ送信する。ステップ 200 ~ 206 はクライアントにより実行され、ステップ 206 ~ 216 はサーバにより実行される。

ステップ 207 でサーバはメッセージを受信する。ステップ 208 でサーバはメッセージから署名 306 を取り除く。署名 306 は図 3E に示すようにメッセージから取り除かれる。

ステップ 209 では、サーバはサーバによって生成、記憶されていたセッションキー（有効ユーザにより生成、記憶されたのと同じセッションキーであるべきである）をメッセージに事前追加する。メッセージにサーバ側セッションキー 304' が事前追加されている図 3F に示されている。決定ブロック 210 では、引き数「64 バイトか？」を形成する。引き数が偽であれば、システムはステップ 211 へ進み、図 3F のパディング 305 により示すように、メッセージの残る部分を零によって充填する。

ステップ211の後、すなわち、決定ブロック210における引き数が真である場合には、システムはステップ212へ進む。ステップ212では、MD4アルゴリズムを実行して、ここではダイジェスト'と呼ばれるサーバメッセージダイジェストを作成する。この結果、図3Gの16バイトのメッセージダイジェストが得られる。このメッセージダイジェストの初めの8つのバイト、すなわち、署名'306'も次に取り除き、クライアントによりメッセージと共に送信されていた署名306と比較する。

決定ブロック213では、引き数「署名=署名'か?」を形成する。このステップは、クライアントにより生成された署名がサーバにより生成された署名'と同じであるか否かを判定するためのものである。決定ブロック213における引き数が真であれば、システムはステップ214へ進み、有効メッセージが示される。ステップ215では、そのメッセージを実行する。決定ブロック213にお

ける引き数が偽であれば、システムはステップ216へ進む。ステップ216では、無許可メッセージを指示し、そのメッセージを廃棄する。ステップ217では、無許可メッセージが試みられたことを指示するために警報を生成する。

本発明の好ましい実施例はダイジェストの8つのバイトを署名として利用する。署名としては、本発明の範囲から逸脱することなく、ダイジェストの任意の数のバイト又はビットを使用して良い。

場合によっては、メッセージパケットは8バイトのメッセージダイジェストを追加する能力を除外して、データフィールド全体を使用する。典型的なアプリケーションにおいては、ブロックサイズ折衝はプロトコルヘッダー情報に対して64バイトを想定する。現実には、大半のプロトコルヘッダーが消費するバイトは56バイト未満であるので、8バイトのダイジェスト情報のために常に利用可能な8つのバイトが残される。8バイトの空きスペースを利用できなければ、8バイトのスペースを保証できるように人為的により小さくしたブロックサイズを折衝する。

#### 状態追跡

先に説明したメッセージ署名方式に加えて、本発明は状態情報を使用するメッ

セージ認証の方法をも提供する。MD 4 アルゴリズムは、それが累積的である、すなわち、メッセージダイジェスト機能を複数の段で実行できるような性質のものである。

たとえば、メッセージのファイルの1つのブロックをメッセージダイジェストアルゴリズムに提供して、ダイジェスティングすることができ、ファイルの次のブロックを読み込み、ダイジェスティングを継続して行くことができる。ダイジェスティングアルゴリズムの実行の出力状態は次のダイジェスティングステップにおける入力状態として使用される。複数の段におけるメッセージダイジェストアルゴリズムを実行することの正味の効果は、メッセージダイジェストアルゴリズムが情報の1ブロック全体を1回のパスで実行するかのようなものである。すなわち、その都度アルゴリズム実行の終了時の状態を覚えておくことによって、累積効果が得られる。本発明はこの累積効果と状態情報を利用して、追加レベルの機密保護と認証を与える。

クライアントとサーバは共に状態情報を追跡し且つ記憶する。本発明では、この状態情報は最も近い時点で生成されたメッセージダイジェストから構成されている。現在メッセージダイジェストと新たなメッセージを使用して、仮メッセージダイジェストがクライアント及びサーバによって生成、記憶される。新たなメッセージが受信されると、新たなメッセージダイジェストを生成して、仮ダイジェストと比較する。他方の相手方が先行状態情報を有していた場合に限り一致が可能である。正しくない開始状態情報は、侵入者と偽造メッセージを識別する誤りを伝搬させる。

図4を参照すると、クライアントに関わる状態追跡の流れ図が示されている。ステップ401では、クライアントの現在状態は先の有効メッセージから生成された全16バイトのメッセージダイジェストである。ステップ402では、クライアントは新たなメッセージを生成する。ステップ403では、現在状態(ダイジェスト)を仮状態を作成するための開始点として使用して、クライアントはメッセージダイジェスティングアルゴリズムを新たなメッセージに適用する。

ステップ404では、メッセージをサーバへ送信する。ステップ405では、



クライアントはサーバからの応答を受信する。ステップ406では、ステップ403の仮状態を使用して、その応答を検査する。これは、メッセージからサーバ側で生成されたダイジェストを取り除き、(開始点として仮状態を使用して)メッセージダイジェストアルゴリズムをメッセージに適用し、その結果得られたダイジェストの初めの8つのバイトをサーバ側で生成されたダイジェストの初めの8つのバイトと比較することによって実行される。

決定ブロック407では、引き数「有効応答か?」を形成する。引き数が偽であれば、システムはステップ408へ進み、無効応答が受信されているために状態を進ませない。クライアントにより生成される次のメッセージは、ダイジェスティングアルゴリズムに関わる開始点として既存の現在状態を使用する。決定ブロック407における引き数が真であれば、システムはステップ409へ進み、状態を進ませる。すなわち、仮状態を現在状態にする。ダイジェスティングアルゴリズムを次のメッセージに適用するとき、その新たな現在状態は開始点となる。

場合によっては、クライアントはデータのバーストをサーバへ送信するかもしれ

ないし、あるいは、クライアントはバースト応答を生成するかもしれない。(第1の packets を除き) packets バースト中のメッセージの順序は必ずしも固定していない。ダイジェスティングアルゴリズムが累積的な性質であるため、これによって状態情報の計算時に問題を引き起こす可能性がある。packets バースト応答に対して、サーバは第1の応答 packets についてメッセージダイジェストを計算し、同じ状態を使用して、バースト中の残る全ての packets についてメッセージダイジェストを計算する。このように、第1の packets の後の packets の順序にかかわらず、状態の保全性を維持できるのである。

バースト要求は同様に処理される。ストリーム中の第1の packets はダイジェストアルゴリズムの状態でくり出しされる。バースト要求の中の後続 packets は初期状態として第1の packets と同じ状態を使用する。

状態情報を維持するときのサーバの動作を表わす流れ図を図5に示す。ステップ501では、サーバはクライアントからのメッセージを受信する。決定ブロッ

ク502では、引き数「バーストか？」を形成する。引き数が真であれば、システムは第1の packets の状態を使用し、ステップ503に戻る。引き数が偽であれば、システムはステップ503へ進み、シーケンス番号を検査する。決定ブロック504では、引き数「繰返しシーケンス番号か？」を形成する。これは繰返し要求を識別するためのものである。要求 packets に対して生成されたダイジェスト出力は常にダイジェスト状態へくられる。すなわち、繰返し要求が現れたときには、サーバにより先のダイジェスト状態を維持しなければならないのである。決定ブロック504における引き数が真であれば、システムはステップ505へ進み、新たなメッセージに基づき、記憶されていた先行状態を使用して仮状態を再計算する。

決定ブロック506では、引き数「バーストか？」を形成する。引き数が真であれば、システムは第1の packets の状態を使用するステップへ進み、ステップ507に戻る。引き数が偽であれば、システムはステップ507へ進む。ステップ507では、仮状態に基づいてメッセージの署名を検査する。決定ブロック508では、引き数「有効か？」を形成する。引き数が偽であれば、システムはステップ509でメッセージを廃棄し、偽造のおそれのあるメッセージに関して警

報を発生する。決定ブロック508における引き数が真であれば、ステップ510でシステムはメッセージに対し応答する。

決定ブロック504における引き数が偽であれば、システムは決定ブロック511へ進む。決定ブロック511では、引き数「次に連続するシーケンス番号か？」を形成する。引き数が偽であれば、システムはステップ512へ進み、メッセージを無効と宣言し、それを廃棄する。言い換えれば、シーケンス番号は不適切だったのである。決定ブロック511における引き数が真であれば、システムはステップ513へ進み、維持されていた仮状態に基づいて署名を検査する。

決定ブロック514では、引き数「有効か？」を形成する。引き数が偽であれば、システムはステップ509へ進み、メッセージを廃棄し、且つ警報を生成する。引き数が真であれば、システムはステップ515へ進む。ステップ515では、仮状態を現在状態として再定義する。ステップ516では、応答に基づいて

新たな仮状態を作成する。決定ブロック517では、引き数「バーストか？」を形成する。引き数が真であれば、システムは第1のバケットの状態を使用し、ステップ518へ進む。引き数が偽であれば、システムはステップ518へ進み、計算されていた仮状態に基づいてクライアントに応答する。

#### セッションキー

クライアントセッションキーを生成する方法を図6に示す。ユーザがネットワークを介して通信することを試みるとき、まず、サーバに対してユーザを識別しなければならない。セッションを開始するために、ユーザはクライアントマシンにログオンしようとする。ステップ601では、クライアントはサーバマシンからの呼掛けを要求する。呼掛けは8バイト分の乱数から構成されている。そこで、クライアントは、ステップ602で、ユーザに対してアカウント名とパスワードを求める。ユーザがアカウント名とパスワードを入力すると、クライアントマシンはステップ603でそのアカウントと関連するオブジェクトIDを確定する。(オブジェクトIDは、各アカウントと関連する数字代理キー、すなわち、索引である。)

ステップ604では、クライアントマシンはパスワードとオブジェクトIDを使用して、ここではDigest1と呼ばれる16バイトの結果を生成するため

にダイジェストアルゴリズムを使用してダイジェストを計算する。ステップ605では、クライアントマシンはDigest1と、呼掛けと、オプションとしてのテキストストリングとのバッファを構成する。好ましい実施例では、本発明のテキストストリングは「許可ネットウェアクライアント」である。ダイジェストアルゴリズムの実行に際して64のバイトを形成するために、必要に応じてバッファに0をパディングする。

ステップ606では、Dbufferと呼ばれるバッファのダイジェストを生成するために、クライアントマシンはバッファについて第2のダイジェスト(Digest1、呼掛け、0のパディング及びオプションとしてのテキストストリング)を実行する。ステップ607の後、Dbufferの初めの8つのバイトを取り除き、セッションキーとして定義する。本発明の好ましい実施例ではセッ

セッションキーとして8バイトを使用するが、本発明の範囲から逸脱することなく任意の数のバイト又はビットを使用して良い。

サーバはユーザのパスワードと、アカウント名と、オブジェクトIDをも記憶している。サーバは呼掛けをも生成しており、その値を記憶する。サーバマシンは同一のステップを使用して、セッションキーを生成することができる。すなわち、セッションキーがワイヤを介して送信されることは決してない。それはクライアントマシンとサーバマシンにおける機密情報から生成される。加えて、セッションキーは1つには呼掛け(乱数)によって決まるので、セッションキーはクライアント/サーバセッションごとに異なる。

図6には示されていないが、呼掛けに対して応答はステップ604の後で生成される。ワイヤを介してサーバへ送信される応答は、ステップ605及び606で使用されるハッシングアルゴリズムとは異なるハッシングアルゴリズムによって生成される。MD4アルゴリズムを使用してステップ604を実行する場合には、呼掛け応答は、たとえば、MD5アルゴリズムを使用でき、セッションキーはMD4アルゴリズムを使用して生成される。あるいは、MD4アルゴリズムを使用して呼掛け応答を生成することができ、MD5アルゴリズムなどの異なるアルゴリズムを使用してセッションキーを生成することが可能である。一方のアルゴリズムの出力から他方のアルゴリズムの出力へのマッピングがない限り、別の

どのようなダイジェスティング方式又はハッシング方式でも使用できる。

MD5アルゴリズムは、本明細書に参考として取り入れられているRFC1321, 「The MD5 Message-Digest Algorithm」, R. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc. 1992年4月の中に説明されている。

#### セッションキー認証

図7は、セッションキーを認証する方法の流れ図を示す。ステップ701では、クライアントは図6に関連して説明したようにしてセッションキーを生成する。ステップ702では、図2に関連して説明したようにダイジェストと署名を生

成するためにセッションキーを使用して、クライアントによりサーバへ要求を送信する。

ステップ 703 では、サーバはクライアントのメッセージから署名を取り除き、サーバ側に記憶されているアカウント名、パスワード及びオブジェクト ID のコピーを使用して、まず、その Digest 1 のバージョン、すなわち、Digest 1' を生成し、次に Digest 1' を使用して、セッションキーのサーババージョン、すなわち、セッションキー' を生成する。ステップ 704 では、サーバは図 2 に関連して説明したように Digest' を生成する。

決定ブロック 705 においては、引き数「署名＝署名' か？」を形成する。引き数が偽であれば、システムはステップ 706 へ進み、サーバは否定の ack (応答) をクライアントへ送信し、サーバはその状態を変えない。サーバは新たなセッションに際してその状態を初期設定しない。決定ブロック 705 における引き数が真であれば、システムはステップ 707 へ進み、サーバは「OK」の肯定応答をクライアントへ送信する。ステップ 708 では、サーバはクライアント状態を初期設定し、サーバが生成したセッションキーを記憶する。ステップ 709 では、サーバはサーバ状態を初期設定し且つセッションキーを記憶する。クライアントとサーバの初期状態は、たとえば、MD 4 規格で文書化されている初期状態であるとして定義される。

本発明のクライアント及びサーバは任意の従来通りのコンピュータシステム又

は汎用コンピュータシステムで実現されれば良い。本発明を実現するためのコンピュータシステムの一実施例の一例を図 8 に示す。キーボード 810 及びマウス 811 は両方向システムバス 818 に結合している。キーボードとマウスはコンピュータシステムにユーザ入力を導入し且つそのユーザ入力を CPU 813 へ通信するためのものである。図 8 のコンピュータシステムはビデオメモリ 814 と、主メモリ 815 と、大容量記憶装置 812 とをさらに含み、それらは全てキーボード 810、マウス 811 及び CPU 813 と共に両方向システムバス 818 に結合している。大容量記憶装置 812 は、磁気記憶システム、光学記憶システム又は磁気光学記憶システム、あるいは他の何らかの利用可能な大容量記憶技術

などの固定媒体と着脱自在な媒体の双方を含んでいて良い。バス818は、たとえば、ビデオメモリ814又は主メモリ815をアドレス指定するためのアドレス線を32本含んでいても良い。システムバス818は、たとえば、CPU813、主メモリ815、ビデオメモリ814及び大容量記憶装置812などの構成要素の間でデータを転送する32ビットデータバスをさらに含む。あるいは、別のデータ線とアドレス線の代わりに、多重データ／アドレス線を使用しても良い。

本発明の好ましい実施例では、CPU813はIntelによって製造されている80386又は80486などの32ビットマイクロプロセッサである。しかしながら、他の何らかの適切なマイクロプロセッサ又はマイクロコンピュータを利用しても良い。主メモリ815はダイナミックランダムアクセスメモリ(DRAM)から構成されている。ビデオメモリ814はデュアルポートビデオランダムアクセスメモリである。

ビデオメモリ814の一方のポートはビデオ増幅器816に結合している。ビデオ増幅器816は陰極線管(CRT)ラスタモニタ817を駆動するために使用される。ビデオ増幅器816は当該技術では良く知られており、何らかの適切な手段によって実現されれば良い。この回路はビデオメモリ814に記憶されている画素データをモニタ817により使用するのに適するラスタ信号に変換する。モニタ817は図形画像を表示するのに適する種類のモニタであり、本発明の好ましい実施例においては、約1020×832の分解能を有する。本発明では他の分解能のモニタを利用しても良い。

以上説明したコンピュータシステムは単なる例示を目的としている。本発明はどのような種類のコンピュータシステム、あるいはプログラミング環境又は処理環境でも実現されうるであろう。

本発明のブロック線図を図9に示す。メッセージ発生器901は送信局から受信局に至るメッセージの供給源である。この例では、送信局はクライアントであり、受信局はサーバである。メッセージ発生器901はメッセージ902を提供する。セッションキー904はセッションキー記憶装置903に記憶されている

。セッションキー904は加算器905でメッセージ902に事前追加され、その結果として追加メッセージ906を得る。追加メッセージ906はダイジェスタ/バッファブロック907に供給されて、そこでダイジェスティングされ、その初めの8つのバイトを署名908として使用する。署名908は加算器911でメッセージ902と組合わされ、その結果として署名付きメッセージ912を得る。署名付きメッセージ912は送受信機913を介して受信局に結合される。

状態記憶装置909は受信局の現在状態と仮状態を記憶しており、それらを線路910を介して必要に応じてダイジェスタ/バッファブロック907に供給する。セッションの初期設定時にセッションキー904を生成するために、呼掛け923と局所パスワード924もダイジェスタ/バッファブロック907に提供される。

受信後の署名付きメッセージ914は減算器915で署名916及びメッセージ917という要素に分離される。メッセージ917は加算器918でセッションキー記憶装置919からのセッションキー920と組合わされ、その結果として追加メッセージ921を得る。追加メッセージ921はダイジェスタ/バッファ922に提供され、そこでダイジェスティングされる。ダイジェストの初めの8つのバイトは署名927を定義する。署名927は、受信メッセージ914の署名916と共に、比較/認証ブロック928に提供される。比較/署名ブロックは署名927を署名916と比較する。署名が一致したとき、有効メッセージを指示する。署名が一致しない場合には、メッセージは無効であると宣言し、メッセージを廃棄する。

ダイジェスタ/バッファ922のダイジェスティング動作のための状態情報は

状態記憶装置925から線路926を介して提供される。呼掛け929とパスワード930も、セッションキーの生成のために、ダイジェスタ/バッファ922に提供される。

図9の要素は処理手段における実行可能な命令として実現可能である。

以上、クライアント/サーバ通信の認証のための方法及び装置を説明した。

【図1】

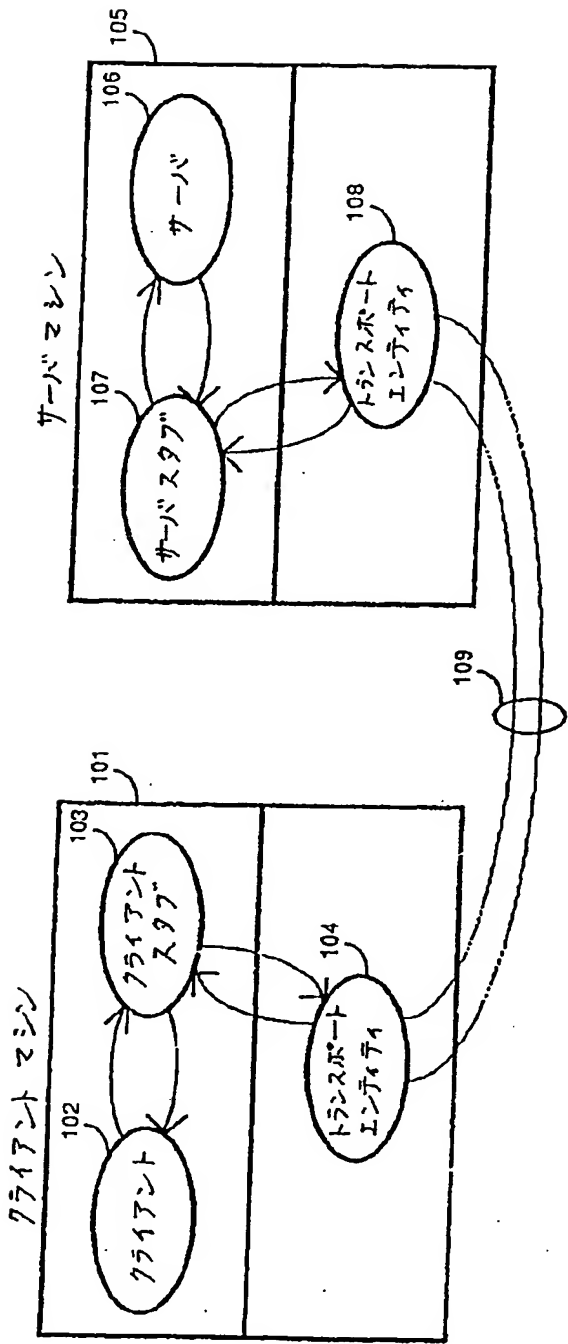
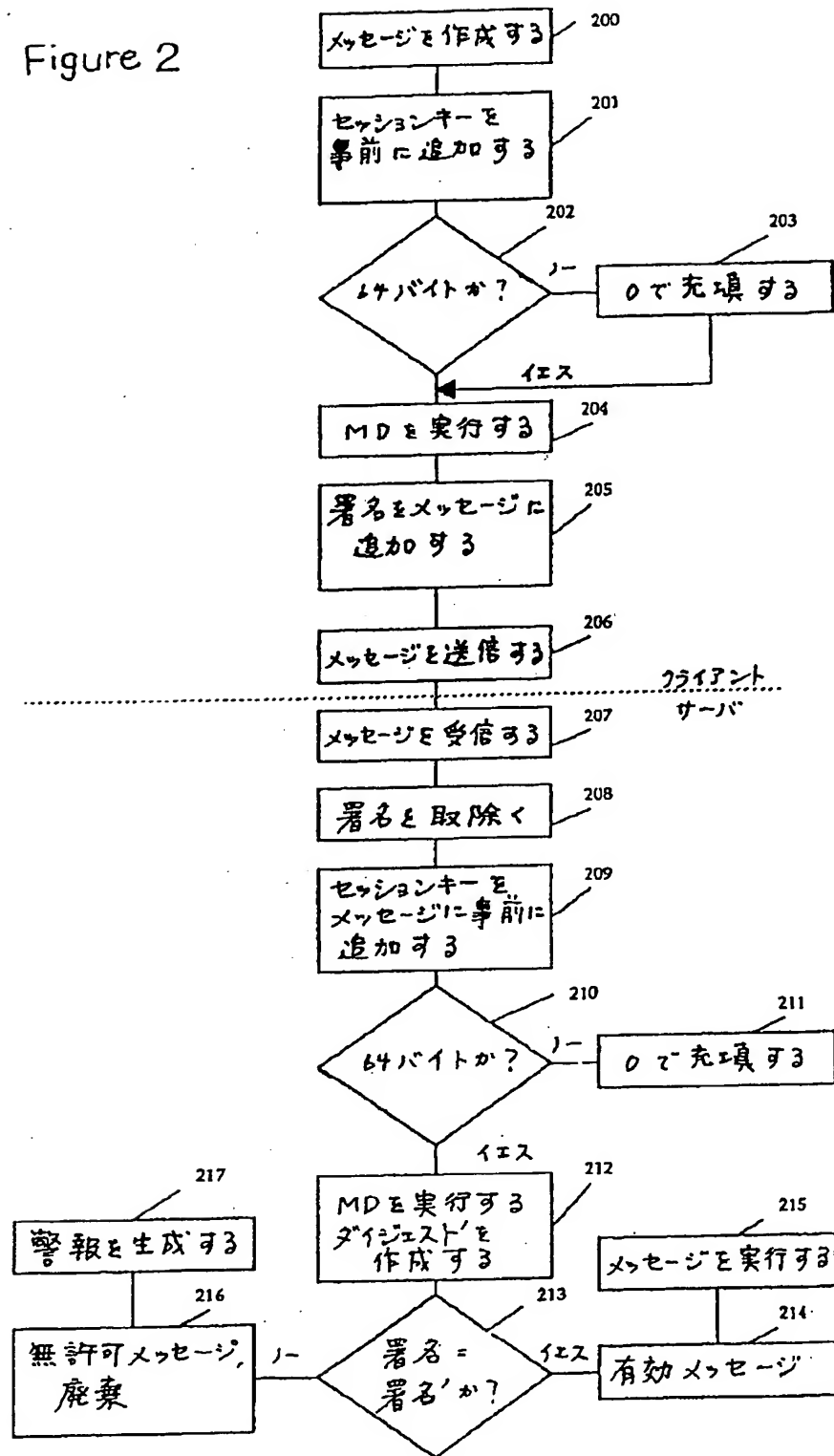


Figure 1

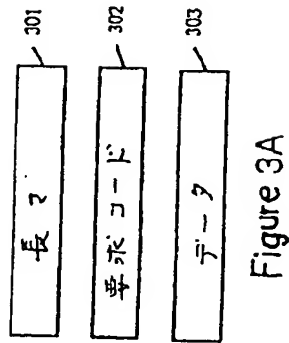


【図2】

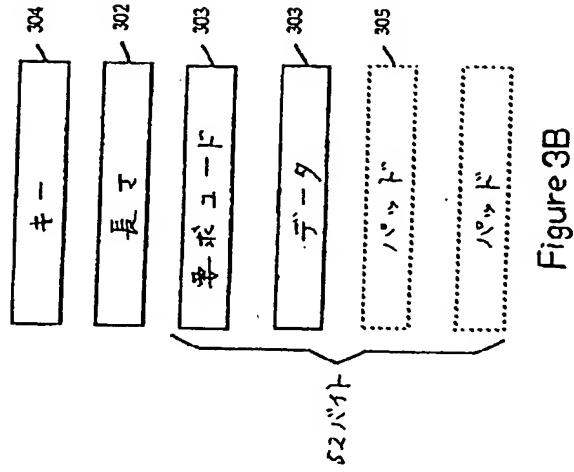
Figure 2



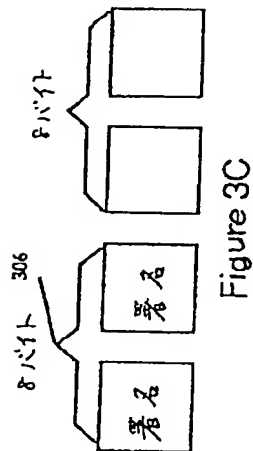
【図 3 A】



【図 3 B】



【図 3 C】



【図3D】

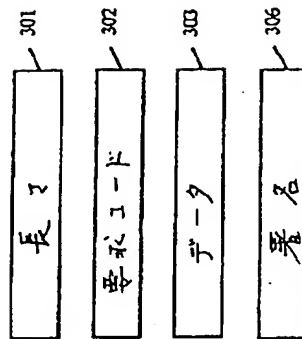


Figure 3D

【図3E】

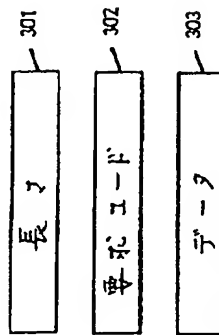


Figure 3E

【図3F】

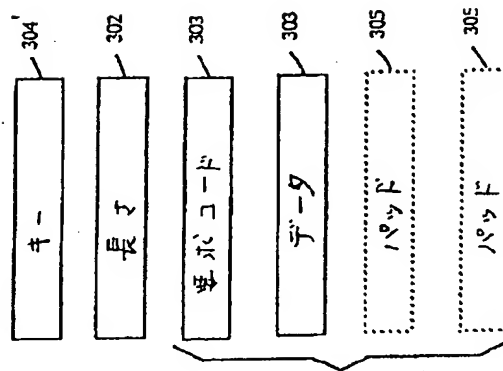
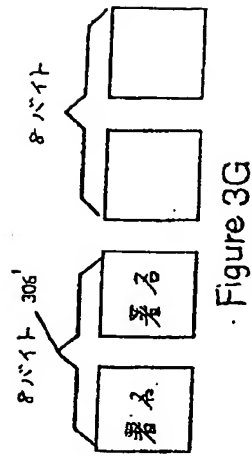


Figure 3F

【図3G】



【図4】

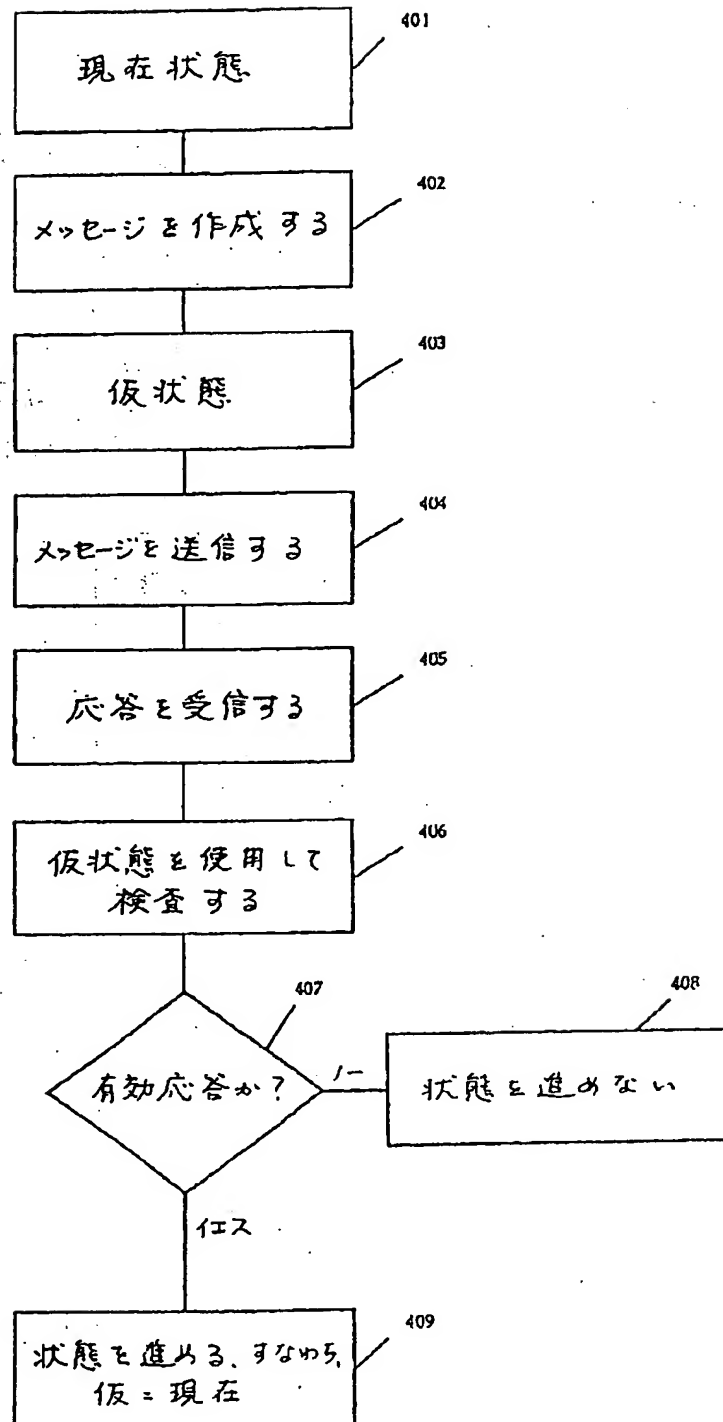


Figure 4

【図 5】

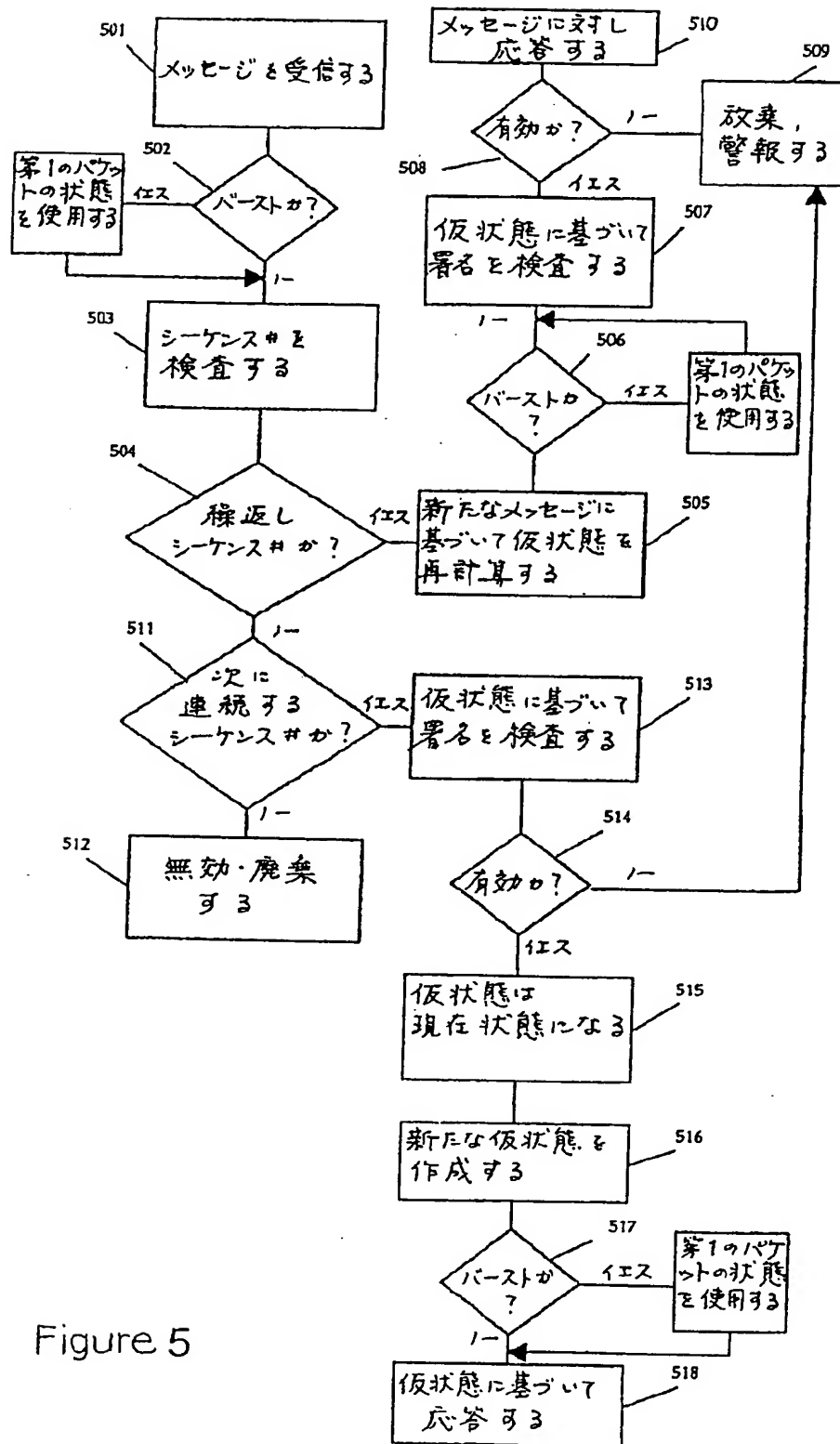


Figure 5

【図6】

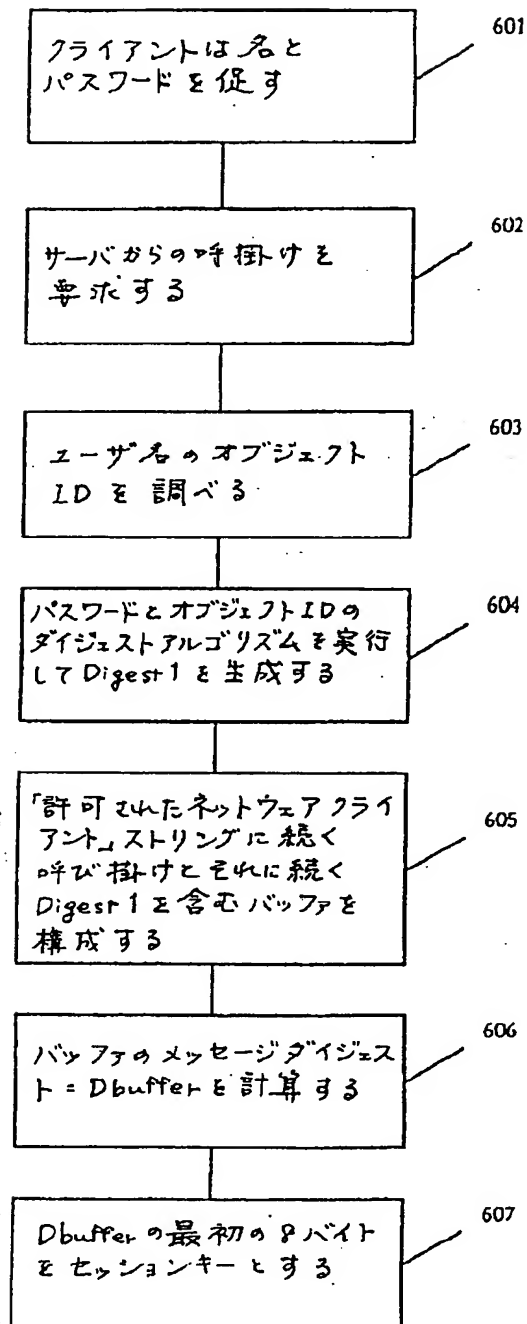


Figure 6

【図7】

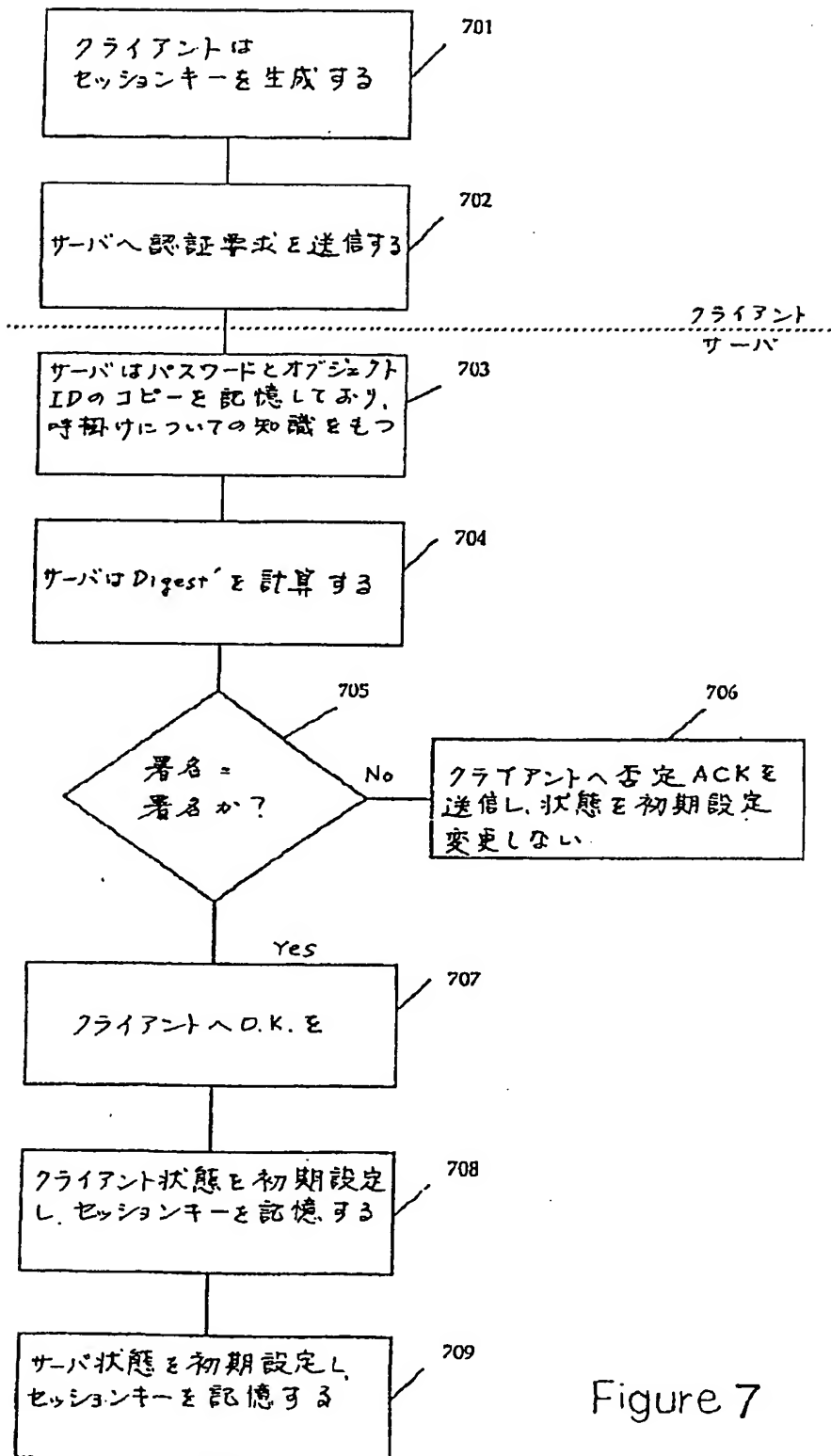


Figure 7



【図8】

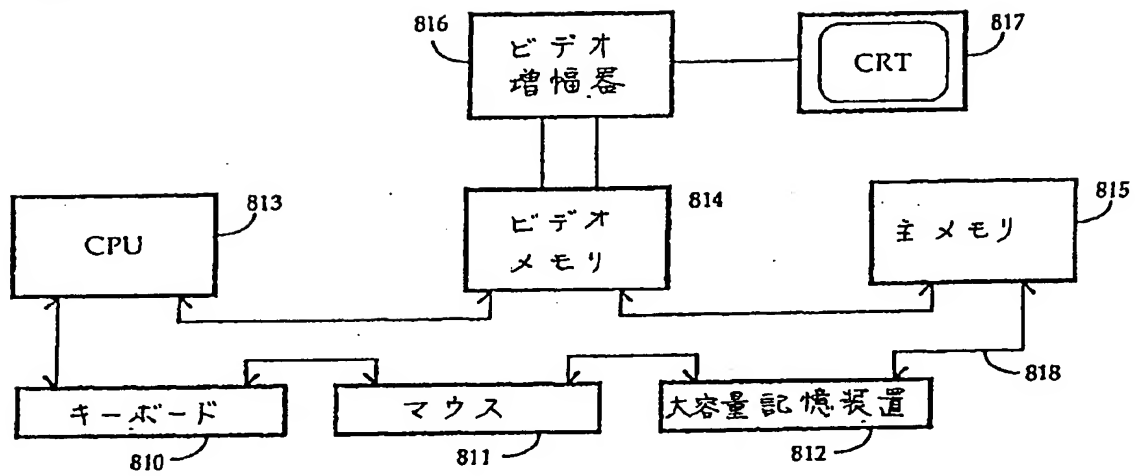


Figure 8

【図 9】

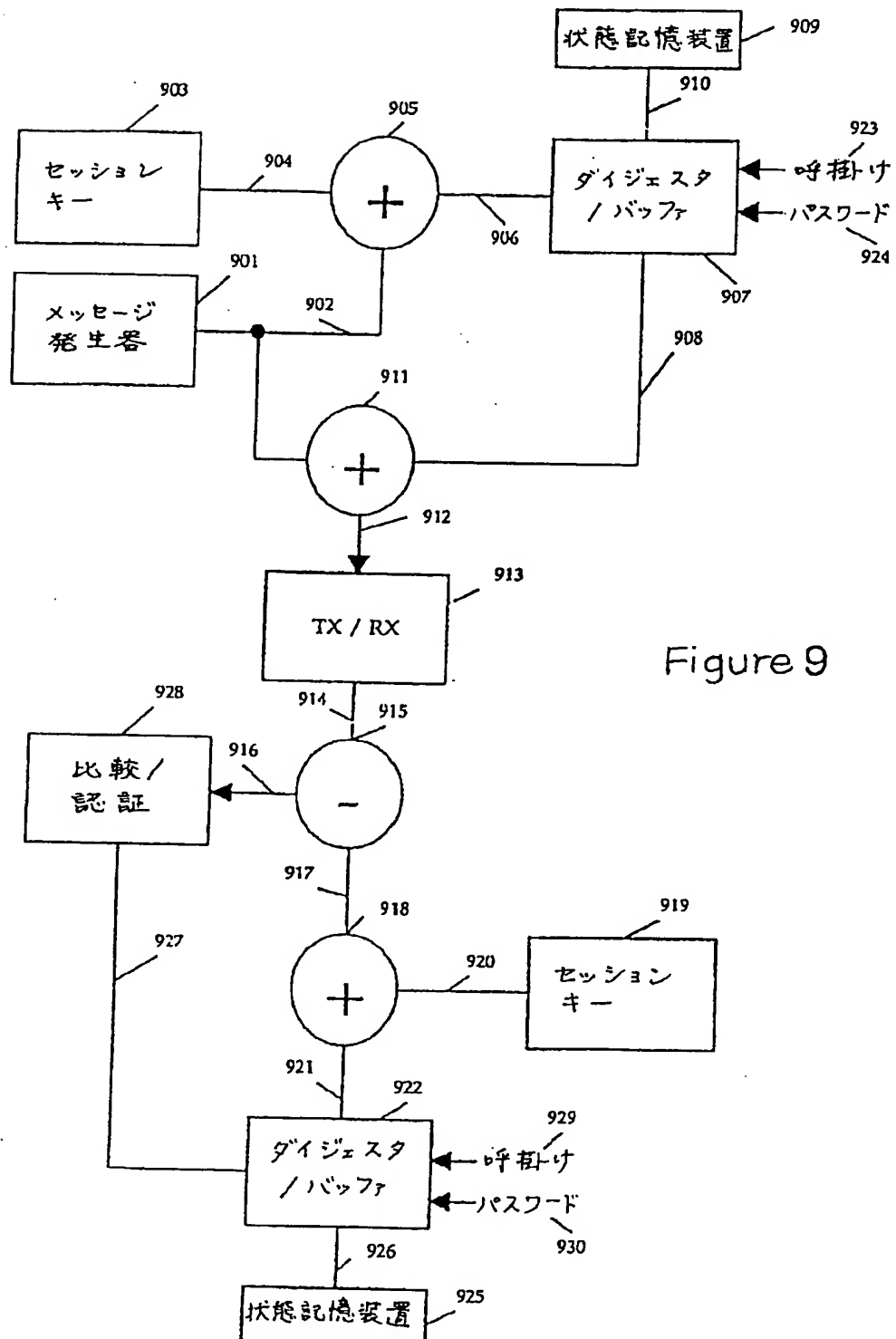


Figure 9

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US93/10585

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) : H04L 9/28

US CL : 380/28

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 25, 28, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,656,474 (MOLLIER ET AL) 07 APRIL 1987, SEE ENTIRE DOCUMENT	1-20
Y	US, A, 4,799,258 (DAVIES) 17 JANUARY 1989, SEE COL. 1, LINES 50-65.	1-20
A	US, A, 4,868,877 (FISCHER) 19 SEPTEMBER 1989, SEE FIG. 5	1-20
Y	US, A, 5,050,212 (DYSON) 17 SEPTEMBER 1991, SEE COL. 3, LINES 15-30.	1-20
Y	US, A, 5,140,634 (GUILLOU ET AL) 18 AUGUST 1992, SEE FIGS. 5 AND 6.	1-20
A,P	US, A, 5,210,795 (LIPNER ET AL.) 11 MAY 1993, SEE FIG. 2.	1-20

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

\* Special categories of cited documents:

\*A\* document defining the general state of the art which is not considered to be part of particular relevance

\*E\* earlier document published on or after the international filing date

\*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reasons (as specified)

\*O\* document referring to an oral disclosure, use, exhibition or other means

\*P\* document published prior to the international filing date but later than the priority date claimed

\*T\*

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\*

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\*

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

\*Z\*

document member of the same patent family

Date of the actual completion of the international search

13 JANUARY 1994

Date of mailing of the international search report

MAR 07 1994

Name and mailing address of the ISA/US  
Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

SALVATORE CANGIALOSI

Telephone No. (703) 308-0482

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AT, AU, BB, BG, BR, BY, CA, CH, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA